Journal of Computer Science

Original Research Paper

Securing IoT Networks: Multi-Attack Detection of RPL Routing Threats Using Deep Learning

Ayoub Krari, Abdelmajid Hajami, Ayoub Toubi and Marouane Ait Said

Laboratory of Research Watch for Emerging Technologies (VETE), Department of Computer Science, Faculty of Science and Technology, Hassan First University of Settat, Settat, Morocco

Article history
Received: 10-09-2024
Revised: 23-10-2024
Accepted: 07-11-2024

Corresponding Author:
Krari Ayoub
Laboratory of Research Watch for Emerging Technologies (VETE), Department of Computer Science, Faculty of Science and Technology, Hassan First University of Settat, Settat, Morocco
Email: ayoub.krari@uhp.ac.ma

Abstract: The growing frequency of cyber threats in Internet of Things (IoT) networks, including attacks on RPL routing, requires the creation of strong detection systems to safeguard network integrity and provide dependable communication. This study is driven by the pressing necessity to tackle the security weaknesses in IoT networks, where threats such as black holes, version number alteration, DIS flooding, and others present substantial threats to the integrity of data and the operation of the network. The main goal of this study is to provide a reliable detection system that can detect and classify ten different RPL routing attacks using machine learning and deep learning methods concurrently. The methodology presented utilizes a Multilayer Perceptron (MLP) model that has been trained and evaluated on a dataset produced by thorough simulations using the Cooja simulator. This dataset encompasses both natural network traffic and diverse malicious actions. The dataset comprises 850,562 transmissions, split equally between 454,781 malicious and 395,801 benign transmissions, covering several attack scenarios. The results indicate that the model has a high level of accuracy, demonstrated by its area under the receiver operating characteristic curve (AUC) of 0.92 and precision-recall area of 0.91. These results successfully differentiate between normal and malicious events. Further confirmation of the model's capacity is provided by the confusion matrix, which demonstrates few false positives and negatives. This study emphasizes the need to create flexible, immediate security measures to strengthen the ability of IoT networks to resist changing cyber risks. This approach establishes a crucial basis for future progress in IoT network security.

Keywords: Cooja, Cyber Threats, Deep Learning, IoT, Intrusion Detection System (IDS), Machine Learning, Multilayer Perceptron (MLP), Multi-Attack Detection, Network Security, RPL Routing Attacks

Introduction

The exponential growth of the Internet of Things (IoT) has drastically transformed several sectors, such as healthcare, smart cities, and industrial automation, by facilitating uninterrupted connection and data interchange across an extensive network of devices (Shafique *et al*., 2020). Nevertheless, this rapid expansion has also made IoT networks vulnerable to a diverse array of cyber risks. Among the various risks, routing attacks that specifically target the IPv6 Routing Protocol for Low-Power and Lossy networks (RPL) are of utmost concern because of their capacity to interrupt network performance, undermine the integrity of data, and enable unauthorized access. Exploiting the weaknesses inherent in RPL, attacks such as black holes, version number modification, DIS flooding, and routing table falsification pose serious threats to the stability and reliability of IoT settings (Sadhu *et al*., 2022).

Even though there is increasing recognition of these risks, current security measures frequently concentrate on identifying a single kind of attack or depend on conventional techniques, such as encryption and firewalls, which are inadequate against the complex, protocol-specific characteristics of RPL attacks. The present study aims to fill a significant void in the existing body of knowledge by introducing a complete detection

framework that has the ability to concurrently detect and classify ten different RPL routing attacks.

This study diverges from other studies that usually concentrate on detecting individual attacks by highlighting a multi-attack detection strategy, therefore offering a more resilient and comprehensive method for safeguarding IoT data networks.

The primary novelty of this study is in the utilization of sophisticated machine learning and deep learning methodologies, particularly a Multilayer Perceptron (MLP) model, to create a flexible security system that can promptly react to various threats in real time. A large dataset built using the Cooja simulator, consisting of over 850,000 communications including both legitimate traffic and a wide spectrum of malicious actions, is used to train and validate the proposed model. The diversity of this dataset guarantees that the model is well prepared to manage different assault scenarios, thereby improving its precision and dependability in practical applications.

This study has two major contributions: Firstly, it showcases the practicality and efficiency of a multi-attack detection approach, so greatly enhancing the existing level of IoT network security. Furthermore, it establishes the foundation for subsequent investigations on adaptive, real-time security systems capable of adapting to evolving threats. This study presents a comprehensive framework for detecting many RPL routing attacks concurrently.

Related Works

It has been studied how to secure the Routing Protocol for Low-power and lossy Networks (RPL) in industrial IoT contexts. As described in Table (1) these approaches have focused on recognizing and mitigating RPL threats such blackhole, version number, and DIS flooding. Recent research has used machine learning, deep learning, and simulation-based methods to identify and mitigate these hazards. Despite their contributions to IoT security, these efforts sometimes have limitations, such as restricted evaluation metrics, attack simulations, and attack detection. A unique machine learning-deep learning methodology is introduced in this study to expand research. The dataset is used with 10 RPL routing attacks and ordinary RPL traffic to create more comprehensive and adaptable security measures. This research advances RPL network security by fixing previous mistakes and prioritizing feature engineering, protecting IoT ecosystems from critical attacks.

Proposed Approach

The proposed security framework as shown in Figs. (1-2) for an IoT network architecture using the Routing Protocol for Low-Power and Lossy Networks is shown in the illustration. Intrusion Detection Systems (IDSs) are key to the multi-attack detection process.

The RPL IoT ROOT Node manages TCP/IP traffic for the network. Network connectivity and data communication depend on this management.

The network relies on many RPL IoT Nodes for RPL communications. The method targets security vulnerabilities like the red Attacker IoT Node.

This node is essential to the framework's ability to detect and stop unsafe data transmissions that threaten network security (Krari *et al*., 2023).

The solution uses a traffic sniffer. Monitoring network traffic for anomalies and odd patterns that may indicate security breaches is crucial. The proposed architecture's Multi-Attack Detection Process module relies on the IDS next to the Traffic Sniffer. It analyzes traffic data to identify and address cyber threats.

The architecture improves IoT network security without increasing communication overhead or device computational needs.

This strategic design keeps the network efficient and the devices sustainable under IoT power limits. The following subsection of the paper will describe the IDS's Multi-Attack Detection Process features and benefits.

Table 1: Simulation environment 1 configuration

Work	Methodology used	Used dataset	Work limitations
Momand *et al*. (2021)	Machine learning (SVM, PCA)	Complex dataset created using Cooja Simulator	No attack simulations, limited evaluation metrics, and only 3 attacks detected
Cakir *et al*. (2020)	Deep learning (GRU)	Datasets starting with "SSN" created in Contiki OS / Cooja Simulator	Only one attack was detected, no details about attack simulations, and limited details about the generated dataset
Belavagi and Muniyal (2020)	Machine learning	No dataset used	Nodes' energy impacted, limited details about attack simulations, 4 possibly detected attacks.
Zahra *et al*. (2022)	Machine learning (Light Gradient Boosting Machine)	Self-generated dataset	Only 2 attacks detected limited attacks impact analysis and limited dataset details.
The proposed work	Deep learning techniques (MLP)	Multi-attacks dataset for the detection of 10 different RPL routing attacks	-

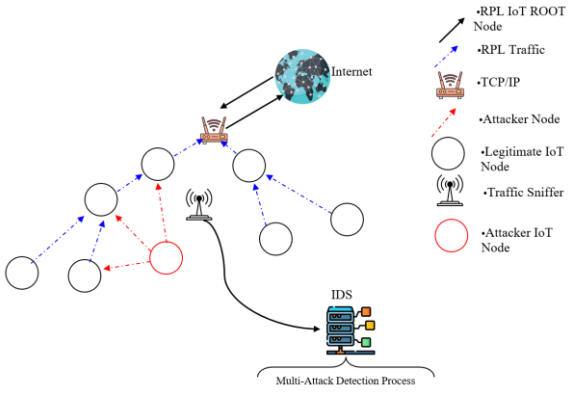

Fig. 1: Multi-attack detection methodology

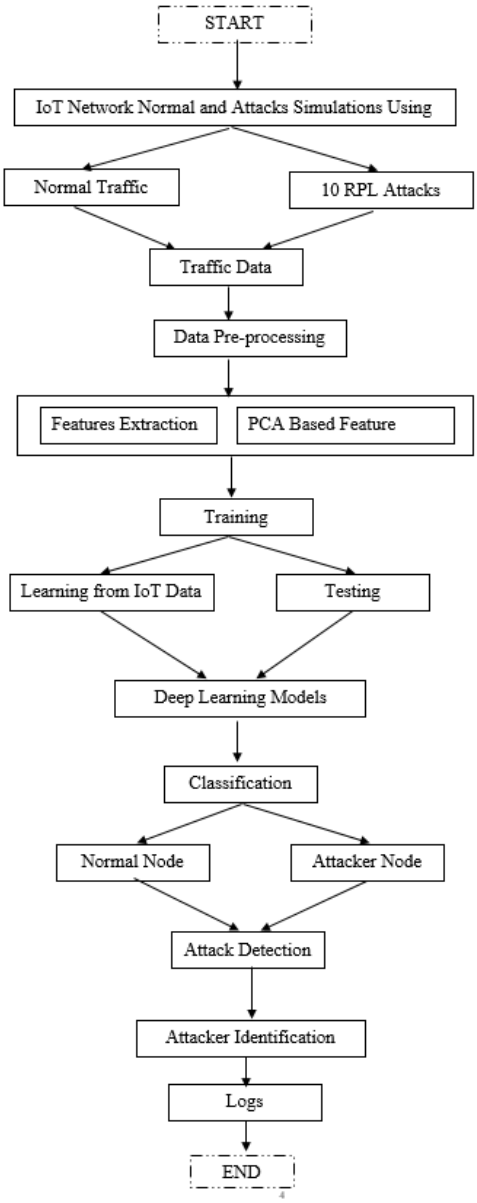

Fig. 2: Multi-attack classification process

Materials and Methods

A complete assessment of the RPL multi-attack detection framework has been performed by conducting extensive simulations as shown in Table (3) designed to mimic real-world IoT network situations. Datasets have been built from simulations that replicated both benign and malicious traffic events.

This study presents a comprehensive dataset that encompasses routine network traffic as well as several attack scenarios, including black holes, selective forwarding, sinkholes, routing table overload, DIS flooding, DAO flooding, DIO flooding, version number, and rank attacks. The Cooja simulator was utilized to build this dataset. The specific makeup of various traffic scenarios is displayed in Table (2), based on the quantification of malicious and benign packets for each type of attack.

The simulations, together with the underlying dataset, will be utilized to train and verify the deep learning models for their efficacy in countering various RPL attacks on IoT networks.

The sample maps show the network topology in both normal and attack scenarios in Figs. (3-4).

Table 2: Simulations configuration

Parameters	Values
Node type	SKY Mote
OS version	Contiki 3.0
Routing protocol	RPL
Radio medium	Unit disk graph
	Medium: Distance loss
OF	MRHOF
Tx Range	50/100 m
Interface range	50/100 m
Simulation area	100×100 m
MTU Size	1280 Byte
Simulation duration	60 min
No. of sender nodes	23
No. of sink node1	1
No. of repetitions	5

Table 3: Simulations scenarios

Scenario	Malicious packets	Benign packets	Total packets
Legitimate	0	100,258	100,258
Blackhotenle	49,116	30,366	79,482
Selective forward	36,614	24,495	61,109
Sinkhole	52,718	35,820	88,538
Routing table overload	34,249	21,102	55,351
DIS flooding	46,914	31,449	78,363
DAO flooding	31,276	20,973	52,249
DIO flooding	45,928	32,272	78,200
Version number	54,070	33,753	87,823
Rank	51,399	33,129	84,528
Routing table falsification	52,477	32,184	84,661
Total	454,781	395,801	850,562

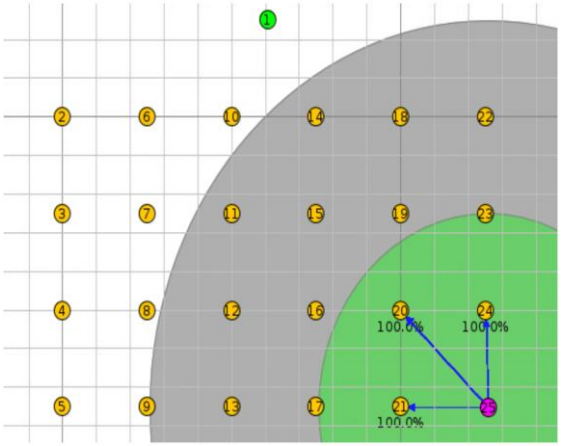

Fig. 3: Multi-attack classification process

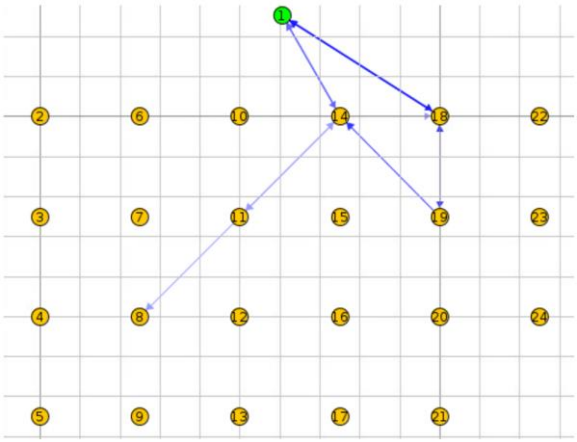

Fig. 4: Multi-attack classification process

Normal Simulation Results

Historical Power Consumption

The power usage as shown in Fig. (5) trends of various IoT nodes over time under normal operating conditions. The graph in Fig. (5) shows the power consumption (in mW) on the y-axis and time on the x-axis, with each line representing a different node in the network.

The data indicates a general trend of high-power consumption initially, followed by a gradual decrease and stabilization over time. This pattern suggests that the nodes experience a higher load at the beginning, potentially due to initial network setup and communication overhead, before settling into a more stable, lower power state.

The variations between the lines also highlight the different power requirements of individual nodes, possibly due to their roles or distances from the network's root node. Understanding these power consumption patterns is crucial for optimizing energy efficiency and extending the lifespan of IoT networks.

Latency

The Latency graph in Fig. (6) indicates the amount of time delay in packet transmission across a network. The flat straight line is always at the top to indicate a low and stable latency value that speaks for the effectiveness and reliability of inter-node communications.

This is the bar chart of the power consumption for each node, broken down into different components: LPM, CPU, radio listening, and radio transmission.

It can be clearly noted that radio listening and transmission activities dominate the major share in consuming power, which is very critical in keeping the network connected and communication alive.

Beacon Interval

The beacon interval graph in Fig. (7) was obtained from the time intervals by which nodes transmitted beacon signals. From the increasing trend in the graph, perhaps there could have been an adaptive mechanism whereby nodes changed their beacon intervals with time for optimum network performance to avoid a lot of collisions.

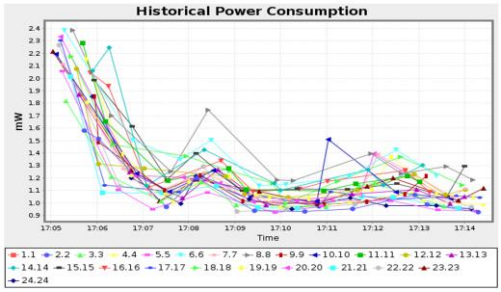

Fig. 5: Historical Power Consumption during normal simulation

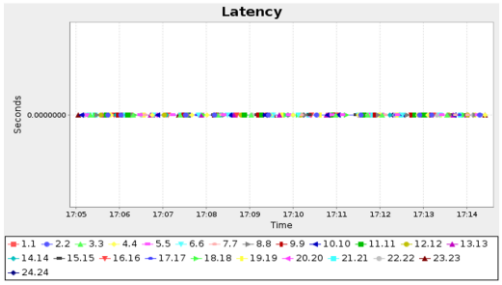

Fig. 6: Latency during normal simulation

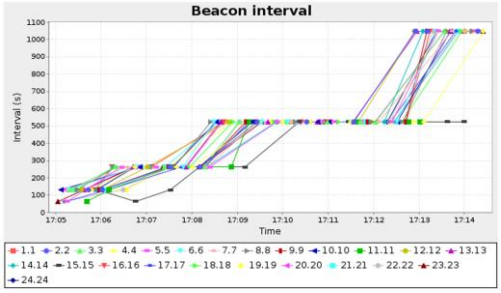

Fig. 7: Beacon interval during normal simulation

Neighbor Count

This graph in Fig. (8) describes the number of neighboring nodes for every node during the simulation.

A consistent count indicates stable network topology and reliable connectivity amongst the nodes (Pushpalatha *et al*., 2021).

Packet Reception

According to the graph depicted in Fig. (9), which shows the total number of packets received, the total number of packets received was 220, with each of the 24 nodes sending out 220 packets. As a result, it is possible to draw the conclusion that there was no loss of packets, which demonstrates that the network is very reliable and efficient while operating under typical circumstances.

Average Radio Duty Cycle

An illustration of the typical radio duty cycle for each node is presented in the form of a bar chart for Fig. (10).

The figure illustrates the percentage of time that the radio is operational for the purposes of transmitting and listening to broadcasts. A duty cycle that is correctly balanced demonstrates that the radio is being utilized in a productive manner.

This indicates that the radio is utilized as little as possible while still delivering sufficient network performance. Therefore, the quantity of energy that is consumed will decrease as a result of this.

Packet Loss

The graph of lost packets that can be found in Fig. (11) provides an indication of the quantity of packets that have been lost in relation to the passage of time.

One interpretation of the flat line at 0 is that it shows that there were no packets lost during the experiment.

This interpretation is possible. This would be an indication of how dependable the network is as well as how resilient the communication is under these circumstances.

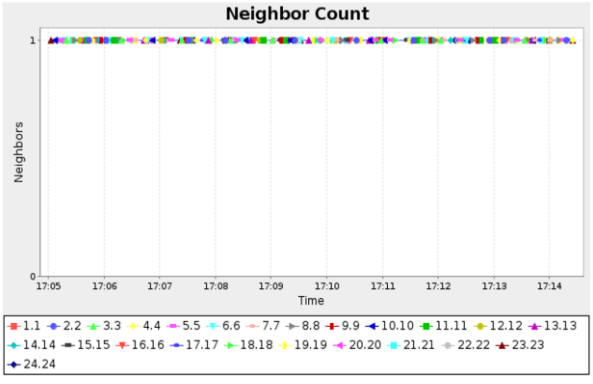

Fig. 8: Nighbor count during normal simulation

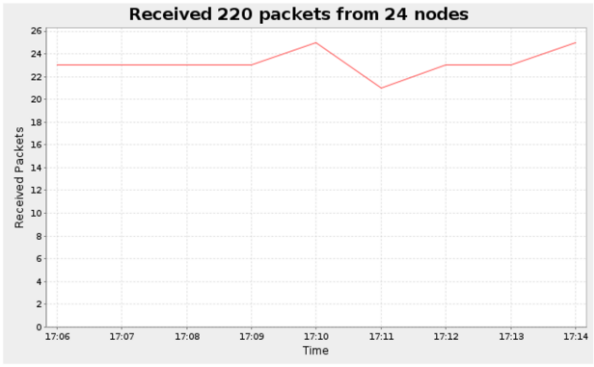

Fig. 9: Received packets during normal simulation

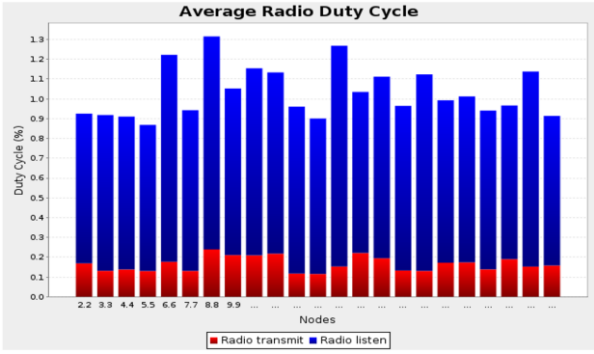

Fig. 10: Average Radio during normal simulation

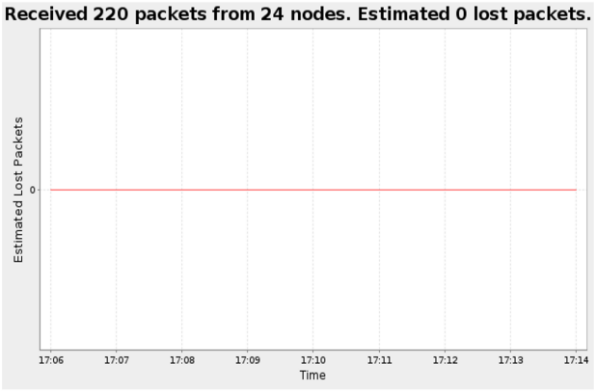

Fig. 11: Packets loss during normal simulation

Simulation Results During Attack Scenarios

The graphs (Figs. 12-14) illustrate various types of attacks on the IoT network, highlighting changes in power consumption, packet loss, and beacon intervals.

The graph in Fig. (12) represents the Instantaneous power consumption by nodes under a flooding attack test indicating a high spike in power consumption, especially in radio listening and transmission activities. Thus, it proves an increase in network activities and load due to flooding.

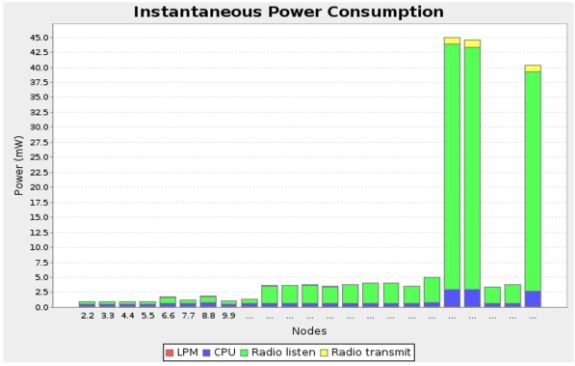

Fig. 12: Power consumption during a flooding attack

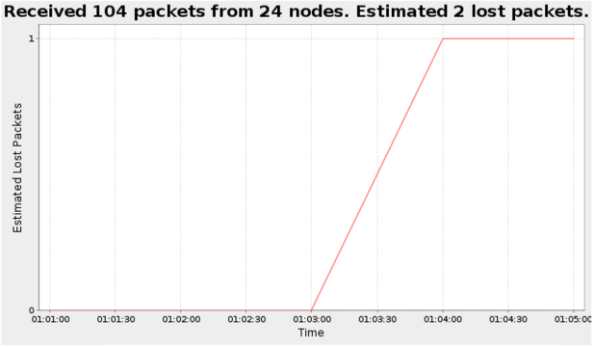

Fig. 13: Packets loss during a blackhole attack simulation

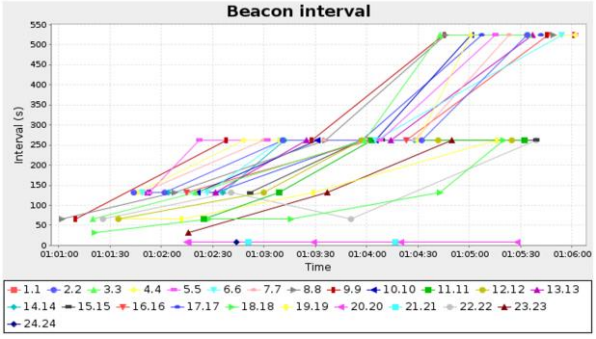

Fig. 14: Beacon interval during attack simulation

The graph in Fig. (13) represents packet loss during the blackhole attack showing that 104 packets were received from 24 nodes and an approximation of lost packets is 2. The steep rise of lost packets corresponds to the disruption caused by the blackhole attack where malicious nodes drop packets instead of forwarding, which causes immense loss in data.

In attacks on the version number, the graph in Fig. (14) shows the beacon intervals in irregular and large intervals, which means a lot of network instability. Nodes are puzzled by frequent topological changes resulting from the malicious manipulation of version numbers; normal network operations are disturbed.

All these results clearly demonstrated the negative effect of certain kinds of attacks on the IoT network's performance. On the other hand, huge changes in power consumption, packet loss, and beacon intervals under different scenarios of attack infer a strong need for efficient detection and mitigation schemes to ensure resilience against attacks and reliability in the operations of networks (Alazab *et al*., 2023).

Features Selection

Table (4) summarizes the key features of common attacks on the RPL protocol. The listed attributes encompass disruptions to the DODAG structure, induced queuing and routing delays, direct packet loss, packet loss via overhead, and the possibility of collaboration and forgery (Alfriehat *et al*., 2024).

This taxonomy helps to enhance comprehension of the methodology of each attack and assists in the categorization and identification of network security mechanisms:

- The blackhole attack is characterized by the malicious node absorbing packets without forwarding them, resulting in direct packet loss. This attack leaves no trace in terms of overhead or delays (Krari *et al*., 2021)
- Selective forwarding is an attack where packets are dropped, resulting in direct packet loss. However, unlike a Blackhole attack, this method does not necessarily impact the DODAG structure or cause delays (Krari *et al*., 2024)
- The sinkhole attack is a deceptive tactic that manipulates network traffic by masquerading a malicious node as the most efficient route. This insidious maneuver disrupts the DODAG structure and can lead to congestion and delays as it attracts an unusually high volume of traffic (Zaminkar and Fotohi, 2020)
- The DAO flood attack aims to compromise the integrity of the DODAG by overloading it with a large number of DAO messages. This flood results in increased overhead and packet loss, which can potentially lead to the dissemination of false routing information and the risk of forgery (Krari *et al*., 2024)
- The overload of the routing table can cause nodes to exceed their capacity, resulting in queuing delays and packet loss. This occurs due to the additional overhead, without directly impacting the transmission of packets (Krari and Hajami, 2024)
- The act of providing inaccurate routing information can result in routing delays and packet loss, which in turn can disrupt the formation of the DODAG network structure, this attack, known as the Version Number Attack, has a significant impact on the DODAG versioning. It results in nodes having outdated or incorrect views of the DODAG structure, which in turn leads to packet loss and potential forgery within the network (Patel, 2022)

- The rank attack compromises the DODAG by advertising a false rank, resulting in routing delays and potential forgery as it misrepresents the node's position in the network hierarchy (Boudouaia *et al*., 2020)
- DIO flooding is a network issue that occurs when an excessive number of DIO messages are sent, causing congestion and packet loss in the DODAG (Krari *et al*., 2024)
- The DIS Flood attack specifically focuses on the DODAG structure by flooding the network with DIS messages. This results in increased overhead and packet loss (Krari *et al*., 2024)

This classification provides valuable insights for the formulation of defensive strategies. By gaining a comprehensive understanding of the network features that each attack targets, security measures can be customized to better detect and mitigate these threats. Considering these attack characteristics is crucial when designing a comprehensive security solution for RPL-based IoT networks.

Features Extraction

The provided Table (5) presents key features crucial to the functionality of the Intrusion Detection System (IDS) in an RPL-based IoT network. The IDS is designed to detect and respond to various threats, highlighting the diverse capabilities of each feature (Garcia Ribera *et al*., 2022).

Presented below is a scholarly analysis of the table, crafted in a concise and academic manner:

- Feature $f1$ is an important indicator for detecting Sinkhole attacks, which involve diverting traffic to a malicious node and anomalies in Rank, where a node falsely advertises its position in the network hierarchy (Omar *et al*., 2024)
- Feature $f2$ helps identify routing table overload, which occurs when there is an excessive propagation of route information, and routing table falsification, which involves the dissemination of corrupt routing information (Popoọla, 2023)
- Feature $f3$ plays a crucial role in identifying two types of attacks: DAO Flooding, which overwhelms the network with excessive route information, and Sinkhole attacks, which involve redirecting traffic to a compromised node. By monitoring the number of DAO messages received, these attacks can be detected (Kumari and Jain, 2023)
- Feature $f4$, the number of DAO messages transmitted, is crucial for identifying DAO Flooding, a potential attack where the network is flooded with an excessive amount of DAO messages (Wadhaj *et al*., 2020)
- Feature $f5$ is an important metric used to detect DIS Flooding attacks, which aim to overload the network with unnecessary solicitation messages (Hamedani, 2023)
- Feature $f6$ is crucial in identifying Blackhole attacks, where packets are dropped, and Selective Forwarding attacks, where only specific packets are forwarded. It plays a vital role in recognizing the count of application packets received (Muzammal *et al*., 2022)
- Feature $f7$, which measures the number of control packets transmitted, plays a crucial role in detecting Blackhole and Selective Forwarding attacks by analyzing outbound traffic (Malik *et al*., 2022)
- Feature $f8$ offers valuable information on the ratio of transmitted to received application packets. It can help identify routing table overload situations, where a significant difference in this ratio may suggest a network that is under excessive strain (Ashraf *et al*., 2021)
- Feature $f9$ is an important attribute for detecting attacks on Rank and Version Number. It is directly linked to a node's reliability and position within the network's topology (Bang and Rao, 2022)
- Feature $f10$, the RPL Version Number is monitored to identify any inconsistencies in version numbers that could indicate potential Version Number attacks targeting the coherence of the DODAG version (Shirafkan *et al*., 2021)

Table 4: Attack features

Attack	DODAG	Queueing delay	Routing delay	Packet loss directly	Packet loss via overhead	Collaboration	Forgery
Blackhole				✓			
Selective forward				✓			
Sinkhole	✓		✓				
DAO flood	✓		✓				
Routing Table Overload			✓		✓	✓	
Routing table falsification	✓					✓	✓
Version Number	✓				✓		✓
Rank	✓		✓				
DIO flood	✓		✓	✓	✓		
DIS flood	✓		✓	✓	✓		

Table 5: Extracted features

#	Features	Attacks detected
$f1$	Number of DIO messages received	Sinkhole, rank, routing table falsification
$f2$	Number of DIO messages transmitted	Routing table overload, routing table falsification
$f3$	Number of DAO messages received	DAO flooding, sinkhole, routing table falsification
$f4$	Number of DAO messages transmitted	DAO flooding
$f5$	Number of DIS messages transmitted	DIS flooding, routing table falsification
$f6$	Number of control packets received	Blackhole, selective forward, routing table falsification
$f7$	Number of application packets transmitted	Blackhole, selective forward
$f8$	The ratio of Transmitted vs received application packets	Routing table overload, routing table falsification
$f9$	Node rank	Rank, version number, routing table falsification
$f10$	Number of RPL version number	Version number

The IDS is designed to effectively detect a broad spectrum of attacks by closely monitoring different aspects of network behavior.

This comprehensive approach enhances the security and resilience of IoT environments, protecting them against sophisticated threats.

Historical Sequence of Feature

In this approach, network traffic is analyzed in discrete time windows to assess the behavior of each node within the network.

Formally, let N represent an RPL network consisting of $|N|$ nodes and let (W_i^t) denote the traffic collected at the i^{th} node, *ni*, during the time window *t*.

The approach constructs a feature set F, consisting of 10 distinct features, to characterize the traffic both quantitatively and qualitatively, as delineated in the referenced Table (5).

The first eight features, f1-8, are quantitative and provide metrics on the volume of traffic, such as the number of received or forwarded control packets (e.g., DIO messages). These features are instrumental in gauging the traffic load managed by each node.

The remaining features, f9-10, are qualitative and offer insights into the status of the node itself, such as its rank in the RPL topology.

Each node's traffic (W_i^t) is then encapsulated into a feature vector F_i^t, which is expressed as:

$$F_i^t = [f1(W_i^t), f2(W_i^t), \ldots, f11(W_i^t)]$$

This vector forms the basis for the analysis, allowing us to apply machine learning or statistical techniques to detect anomalies that may indicate security threats such as intrusion attempts or misconfigurations within the network.

The network representation schema, depicted in Fig. (15), illustrates how each node n maintains its own behavioral history.

These histories exhibit distinct patterns that differ across various features, reflecting the unique operational roles and network positions of the nodes.

Fig. (15) provides an overview of the feature extraction process within the proposed security framework, focusing on the analysis of IoT network traffic. At each discrete time window (W_i^t), a feature vector F_i^t is extracted for every node-*i* in the network. This vector is the culmination of 10 representative features, carefully selected for their relevance in characterizing network behavior and identifying potential security threats.

For each node *i*, the behavior *Bi* is constructed based on the composition of its respective feature vectors F_i^t over time.

These behavioral compositions allow for temporal analysis of network activity, facilitating the detection of anomalies or irregularities that may indicate malicious actions or network vulnerabilities.

The systematic aggregation of these feature vectors enables a robust security posture, allowing for proactive threat detection and response within the IoT network.

In the proposed security framework, the features are extracted from the traffic received at each node to characterize the device's behavior.

For each node *ni*, the extracted feature vector F_i^t encapsulates the quantifiable attributes of the traffic at a given time window *t*. This vector is then sequentially integrated into the behavioral history *Bi* of the node, which is formally represented as:

$$Bi = [F_0^t, \ldots, F_i^t]$$

Sample of Node Behaviors During Attack Scenarios

The historical sequence of feature vectors allows for a comprehensive behavioral analysis over time.

Figures (16-17) provide a visual comparison of behavioral patterns related to the features $f5$ and $f7$ specifically, the number of DIS Messages Transmitted and the number of application packets transmitted. These figures reveal the distinct activity profiles of three nodes, labeled Node 4, Node 21, and Node 9. The depicted patterns reflect the nodes' varying roles and positions within the RPL hierarchy, as modeled in a simulation environment.

In Fig. (16), the fluctuation in the number of DIS Messages transmitted suggests different exposure levels to DIS Flooding attacks, with each node responding according to its unique network context.

Meanwhile, Fig. (17) illustrates the transmission activity of application packets, providing insights into how each node contributes to the network's functionality, potentially indicating susceptibility to Blackhole or Selective Forward attacks.

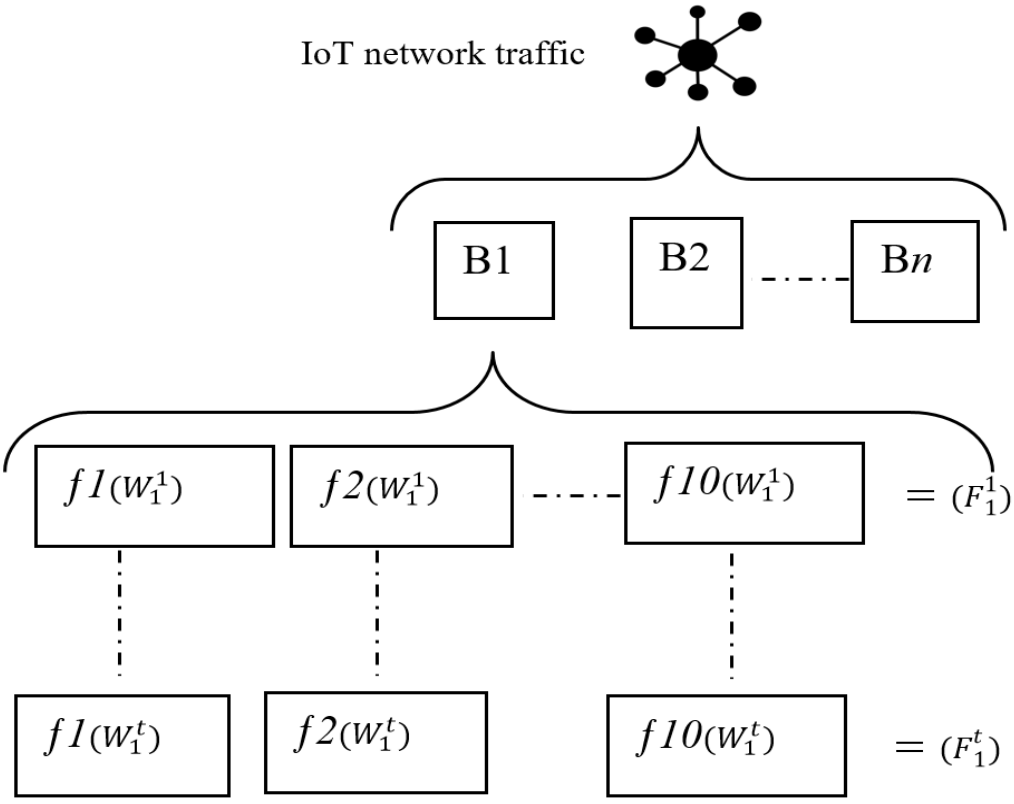

Fig. 15: Historical sequence of nodes' behaviors and features

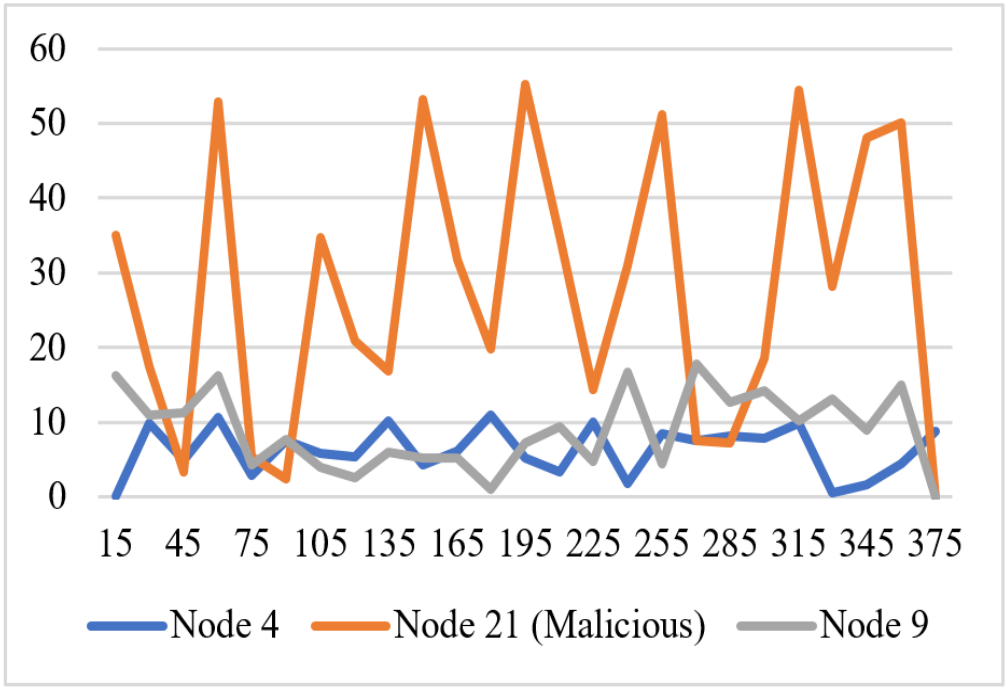

Fig. 16: Number of DIS Messages Transmitted ($f5$)

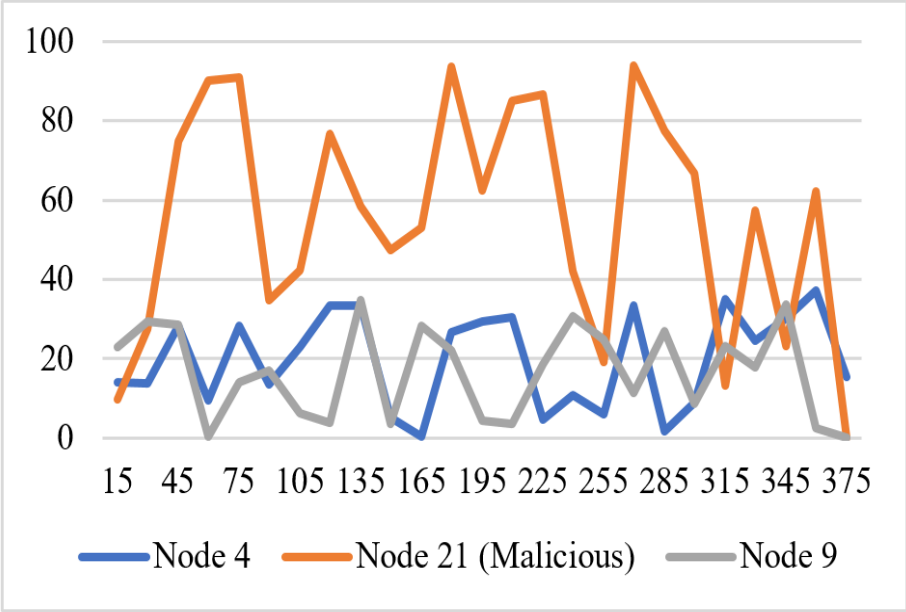

Fig. 17: Number of control packets Received ($f6$)

Table 6: Sample of the dataset

No	Time	Source Node	Destination Node	Length	Info	$f1$	$f2$	$f3$	$f4$	$f5$	$f6$	$f7$	$f8$	$f9$	$f10$	LABEL
1	0.475	15	9999	64	2	10	5	8	7	15	100	150	1.205	9	1	0
2	0.487	25	9999	64	2	11	100	9	6	200	300	400	1.312	10	2	1
3	0.493	2	9999	64	2	9	4	10	8	12	80	120	1.507	11	1	0
4	0.499	25	9999	64	2	12	90	7	5	180	270	360	1.329	12	2	1
5	0.511	8	9999	64	2	10	6	9	7	14	90	130	1.413	10	1	0
6	1.301	25	9999	64	2	11	110	8	6	220	330	440	1.301	9	3	1
7	1.31	7	9999	64	2	9	7	10	8	16	95	140	1.519	11	1	0
8	1.318	25	9999	64	2	12	95	7	5	190	285	380	1.324	12	2	1
9	1.326	15	9999	64	2	10	8	9	7	18	85	125	1.546	10	1	0
10	1.334	25	9999	64	2	11	105	8	6	210	315	420	1.378	9	3	1
11	1.935	2	9999	64	2	9	9	10	8	20	100	150	1.502	11	1	0

The comparative analysis facilitated by these figures highlights the precision of the feature extraction methodology, which successfully identifies and differentiates the operational behaviors of individual nodes in the IoT network.

This differentiation is critical for the accurate detection and classification of potential security threats based on the traffic patterns observed (Table 6).

Results and Discussion

Model Accuracy

The graph in Fig. (18) illustrates the performance of the Multilayer Perceptron (MLP) model throughout 500 epochs, providing valuable insights into its ability to learn and generalize. The training accuracy quickly reaches a high level of approximately 99%, suggesting successful learning from the training data. Nevertheless, the testing accuracy remains consistently at around 90%, with minor fluctuations. This indicates that the model is capable of effectively identifying various RPL routing attacks. However, it is important to note there may be slight variations in its performance when dealing with unfamiliar data. The disparity between the accuracy of the model during training and testing draws attention to a possible overfitting concern. This occurs when the model becomes too focused on learning specific patterns from the training set, which may not be applicable to new data.

Nevertheless, the model's high testing accuracy serves as a strong indicator of its effectiveness in real-world scenarios (Egbueri and Agbasi, 2022). Potential future enhancements involve the implementation of regularization or dropout techniques to improve generalization and further reduce overfitting.

Model Receiver Operating Characteristic ROC

The "Receiver Operating Characteristic (ROC)" graph in Fig. (19) depicts the performance of the Multilayer

Perceptron (MLP) model in differentiating between normal and malicious traffic in Internet of Things (IoT) networks. The Receiver Operating Characteristic (ROC) curve is a graphical representation that illustrates the relationship between the true positive rate (also known as sensitivity) and the false positive rate (Patel *et al*., 2021). This curve serves as a visual indicator of the model's ability to distinguish between different classes or categories. The proximity of the curve to the upper left corner indicates a high level of accuracy, as evidenced by an Area Under the Curve (AUC) value of 0.92. The high AUC value indicates that the model possesses a strong capability to accurately classify both positive and negative cases, thereby reducing the occurrence of false positives and false negatives. The steep ascent of the curve in the direction of the upper left corner indicates that the model exhibits a consistently high rate of correctly identifying positive instances while keeping the rate of incorrectly identifying negative instances low. This demonstrates the model's strength and dependability in accurately detecting various RPL routing attacks in the Internet of Things (IoT) environment.

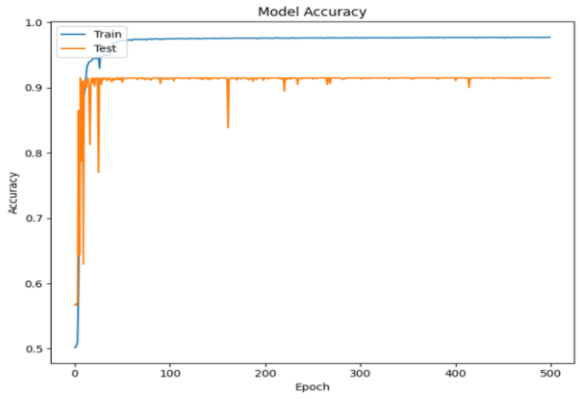

Fig. 18: Model accuracy

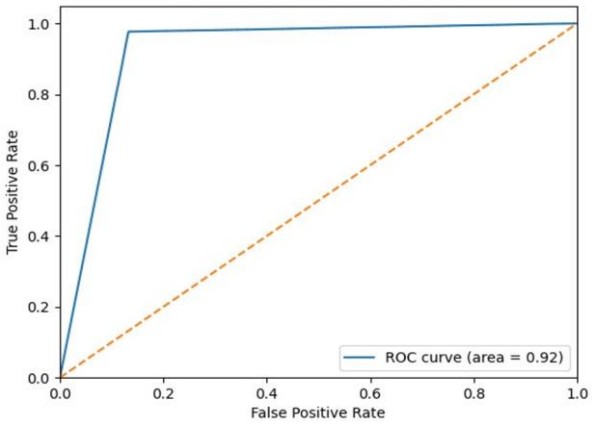

Fig. 19: Model receiver operating characteristic

Model Confusion Matrix

A comprehensive analysis of the classification performance of the Multilayer Perceptron (MLP) model in differentiating between benign and malicious packets in the IoT network is presented in the "Confusion Matrix" graph in Fig. (20).

The matrix indicates that 78,384 true negatives (properly recognized normal packets) and 74,046 true positives (correctly identified malicious packets) were obtained out of the total predictions.

Nevertheless, there were a total of 6,019 false positives, which refer to normal packets that were mistakenly identified as malicious, and 2,024 false negatives, which refer to poisonous packets inaccurately identified as normal.

The model's high true positive and true negative rates demonstrate its robust capability to precisely categorize various forms of network traffic. However, the existence of certain incorrect positive and negative results indicates that there is potential for enhancing the sensitivity and specificity of the model.

The findings validate the model's general efficacy in safeguarding IoT networks, while also emphasizing the need for additional refinement to improve the accuracy of detection.

Model Precision-Recall Curve

A detailed representation of the model's ability to differentiate between true positives and false positives at various thresholds is shown in Fig. (21).

With an Area Under the Curve (AUC) of 0.91, the curve plots recall (the ratio of true positives to the sum of true positives and false negatives) versus precision (the ratio of true positives to the sum of true positives and erroneous negatives).

The achieved high AUC value suggests that the model successfully achieves a favorable equilibrium between precision and recall, hence reducing the occurrence of false positives and maximizing the capture of genuine positives.

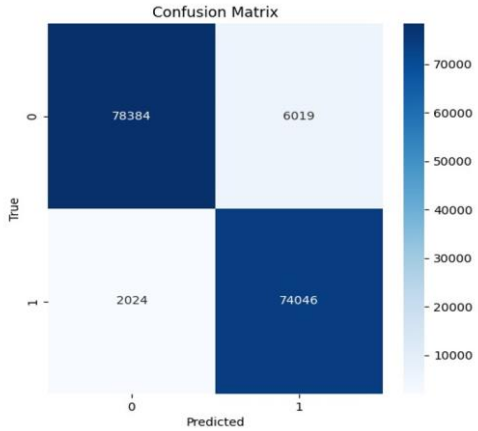

Fig. 20: Model confusion matrix

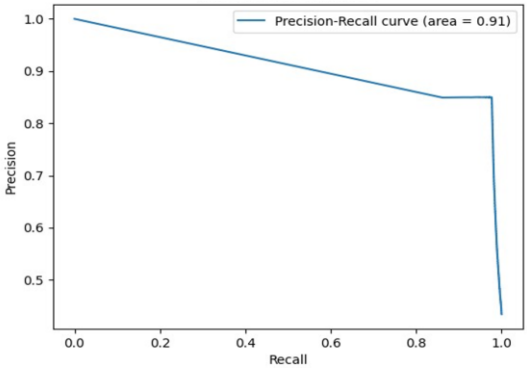

Fig. 21: Model precision-recall curve

The curve exhibits a pattern where the model maintains a high level of precision while recall declines.

However, there is a significant decline towards the end, indicating that the model's capacity to sustain both high precision and recall concurrently is tested under specific circumstances.

The model's high precision-recall AUC validates its efficacy in precisely identifying certain RPL routing exploits in IoT networks.

However, there is still a need for additional refinement to enhance its performance in all situations.

Discussion and Comparison with other Approaches

Various approaches, including the "Proposed Work," are compared in Table (7) to several other methods in their ability to detect a range of RPL routing attacks. Blackhole, Selective Forwarding, Sinkhole, Continuous Sinkhole, DIS Flooding, DAO Flooding, DIO Flooding, Wormhole, Version Number, Rank, Worst Parent, Falsification attacks, and routing table overload are among the attacks being compared. A comprehensive framework is presented to detect many types of attacks.

The exhaustive identification of several attack categories demonstrates the adaptability and resilience of the suggested method in safeguarding IoT networks. Raghavendra *et al.* (2022) provide detection of Blackhole, Selective Forwarding, Sinkhole attacks, as well as Rank attacks. Ioulianou *et al.* (2022) largely examine Blackhole and Rank attacks. Both Pu (2020); Almusaylim *et al.* (2020) address the topics of Rank and Version Number attacks.

The detection of Wormhole and Version Number attacks has been accomplished by Osman *et al.* (2021); Zahra *et al.* (2022). The works of Momand *et al.* (2021); Cakir *et al.* (2020) address the Wormhole vulnerability and exhibit some similarities with rank attacks.

The proposed work exhibits enhanced coverage throughout a wider spectrum of attacks in comparison to alternative approaches. The extensive coverage of the proposed solution enhances its effectiveness in offering robust security against RPL routing attacks in IoT networks.

Table 7: Comparison with other approaches

Attacks	Proposed work	Raghavendra *et al.* (2022)	Ioulianou *et al.* (2022)	Pu (2020)	Almusaylim *et al.* (2020)	Osman *et al.* (2021)	Zahra *et al.* (2022)	Momand *et al.* (2021)	Cakir *et al.* (2020)
Blackhole	✓	✓	✓						
Selective forwarding	✓	✓							
Sinkhole	✓	✓							
Continuous Sinkhole	✓								
DIS Flooding	✓							✓	✓
DAO Flooding	✓								
DIO Flooding	✓								
Wormhole							✓		
Version Number	✓				✓			✓	
Replay									
Rank	✓	✓	✓		✓	✓	✓	✓	
Worst parent									
Falsification Attacks									
Routing table overload	✓								

Conclusion

The present research devised an extensive detection framework for various RPL routing exploits in IoT networks by employing a Multilayer Perceptron (MLP) model. Based upon a dataset produced by thorough simulations, the model successfully differentiated between valid and malicious communications in ten distinct attack scenarios. The model demonstrated excellent performance measures, including a Receiver Operating Characteristic (ROC) Area Under the Curve (AUC) of 0.92 and a Precision-Recall AUC of 0.91. These results indicate its robust capacity to identify attacks with reduced occurrence of false positives and negatives. The observed outcomes highlight the efficacy of the suggested methodology in augmenting the security and dependability of IoT networks against various advanced threats.

In order to enhance the model's generalization capabilities and mitigate overfitting, future research must concentrate on integrating methods such as regularization, dropout, and data augmentation. Additionally, investigating alternative machine learning architectures, such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), could result in additional enhancements in the accuracy and resilience of detection. Incorporating a wider range of attack types and real-world traffic patterns into the dataset would further improve the model's suitability in other IoT domains. Integration of this detection framework with real-time adaptive security systems has the potential to provide enhanced and prompt protection, therefore bolstering the resilience of IoT networks against ever-changing cyber threats.

Acknowledgment

Firstly, I express my deepest gratitude to God for providing me with the fortitude and resilience to overcome all challenges encountered during this research. Secondly, I extend my sincere appreciation to the esteemed members of the Laboratory of Research Watch for Emerging Technologies (VETE), whose contributions, both direct and indirect, have been indispensable to the completion of this manuscript. In conclusion, my heartfelt thanks are particularly directed towards Prof. Abdelmajid Hajami, under whose expert guidance and supervision this study was brought to fruition.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

Ayoub Krari: As the first author and primary investigator, I was in charge of the study's conceptualization and design, led the methodology development, performed the majority of the simulations and data analysis, and wrote the first draft of the manuscript, as well as subsequent revisions.

Abdelmajid Hajami: as the project's supervisory professor, played an important role in setting the project's intellectual orientation, providing vital insights into the research and analysis, and participating in data interpretation. He also helped with the critical revision of the manuscript.

Ayoub Toubi: Helped with data collecting, analytical procedures utilized in the study, and manuscript revision.

Marouane Ait Said: Helped evaluate data, provided insights into the larger research context, and assisted with manuscript editing.

Ethics

The authors confirm that this manuscript has not been published elsewhere and that no ethical issues are involved as the article conforms to all established scientific ethical principles.

References

Alazab, A., Khraisat, A., Singh, S., Bevinakoppa, S., & Mahdi, O. A. (2023). Routing Attacks Detection in 6LoWPAN-Based Internet of Things. *Electronics*, *12*(6), 1320. https://doi.org/10.3390/electronics12061320

Alfriehat, N. A., Anbar, M., Karuppayah, S., Rihan, S. D. A., Alabsi, B. A., & Momani, A. M. (2024). Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy. *IEEE Access*, *12*, 31136–31158. https://doi.org/10.1109/ACCESS.2024.3368633

Almusaylim, Z. A., Jhanjhi, N., & Alhumam, A. (2020). Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP. *Sensors*, *20*(21), 5997. https://doi.org/10.3390/s20215997

Ashraf, U., Ahmed, A., Al-Naeem, M., & Masood, U. (2021). Reliable and QoS-aware routing metrics for wireless Neighborhood Area Networking in smart grids. *Computer Networks*, *192*, 108051. https://doi.org/10.1016/j.comnet.2021.108051

Bang, A. O., & Rao, U. P. (2022). EMBOF-RPL: Improved RPL for early detection and isolation of rank attacks in RPL-based Internet of things. *Peer-to-Peer Networking and Applications*, *15*(1), 642–665. https://doi.org/10.1007/s12083-021-01275-3

Belavagi, M. C., & Muniyal, B. (2020). Multiple intrusion detection in RPL-based networks. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*(1), 467–476. https://doi.org/10.11591/ijece.v10i1.pp467-476

Boudouaia, M. A., Ali-Pacha, A., Abouaissa, A., & Lorenz, P. (2020). Security against Rank Attack in RPL Protocol. *IEEE Network*, *34*(4), 133–139. https://doi.org/10.1109/mnet.011.1900651

Cakir, S., Toklu, S., & Yalcin, N. (2020). RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning. *IEEE Access*, *8*, 183678–183689. https://doi.org/10.1109/access.2020.3029191

Egbueri, J. C., & Agbasi, J. C. (2022). Performances of MLR, RBF-NN and MLP-NN in the evaluation and prediction of water resources quality for irrigation purposes under two modeling scenarios. *Geocarto International*, *37*(26), 14399–14431. https://doi.org/10.1080/10106049.2022.2087758

Garcia Ribera, E., Martinez Alvarez, B., Samuel, C., Ioulianou, P. P., & Vassilakis, V. G. (2022). An Intrusion Detection System for RPL-Based IoT Networks. *Electronics*, *11*(23), 4041. https://doi.org/10.3390/electronics11234041

Hamedani, A. F. (2023). *Scalable and Reliable Framework to Detect and Mitigate DDoS Attack in OpenFlow-based SDN Network*. https://doi.org/10.53846/goediss-10038

Ioulianou, P. P., Vassilakis, V. G., & Shahandashti, S. F. (2022). A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks. *Journal of Cybersecurity and Privacy*, *2*(1), 124–153. https://doi.org/10.3390/jcp2010009

Krari, A., & Hajami, A. (2024). RPL-Shield: A Deep Learning GNN-Based Approach for Protecting IoT Networks from RPL Routing Table Falsification Attacks. *Digital Technologies and Applications*, 117–127. https://doi.org/10.1007/978-3-031-68650-4_12

Krari, A., Hajami, A., & Jarmouni, E. (2021). Study and Analysis of RPL Performance Routing Protocol under Various Attacks. *International Journal on Technical and Physical Problems of Engineering (IJTPE)*, *13*(49), 152–161.

Krari, A., Hajami, A., & Jarmouni, E. (2023). Detecting the RPL Version Number Attack in IoT Networks using Deep Learning Models. *International Journal of Advanced Computer Science and Applications*, *14*(10), 614–623. https://doi.org/10.14569/ijacsa.2023.0141065

Krari, A., Hajami, A., Toubi, A., & Mihi, S. (2024). Securing IoT Networks: A Deep Learning Strategy against RPL Selective Forwarding Attacks. *International Journal of Engineering Trends and Technology*, *72*(8), 197–211. https://doi.org/10.14445/22315381/ijett-v72i8p120

Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, *127*, 103096. https://doi.org/10.1016/j.cose.2023.103096

Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J.-T. (2022). An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. *Sensors*, *22*(5), 1897. https://doi.org/10.3390/s22051897

Momand, M. D., Khan Mohsin, M., & Ihsanulhaq. (2021). Machine Learning-based Multiple Attack Detection in RPL over IoT. *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 1–8. https://doi.org/10.1109/iccci50826.2021.9402388

Muzammal, S. M., Murugesan, R. K., Jhanjhi, N. Z., Humayun, M., Ibrahim, A. O., & Abdelmaboud, A. (2022). A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things. *Sensors*, *22*(18), 7052. https://doi.org/10.3390/s22187052

Omar, A., Soudan, B., & Altaweel, A. (2024). Detecting Sinkhole Attacks in Rpl-Based Iot Networks Using an Optimized Cnn-Mlp Hybrid Model. *SSRN*. https://doi.org/10.2139/ssrn.4855556

Osman, M., He, J., Mohammed Mokbal, F. M., & Zhu, N. (2021). Artificial Neural Network Model for Decreased Rank Attack Detection in RPL Based on IoT Networks. *International Journal of Network Security*, *23*(3), 496–503. https://doi.org/10.6633/IJNS.202105 23(3).15

Patel, A., Cooper, N., Freeman, S., & Sutton, A. (2021). Graphical enhancements to summary receiver operating characteristic plots to facilitate the analysis and reporting of meta-analysis of diagnostic test accuracy data. *Research Synthesis Methods*, *12*(1), 34–44. https://doi.org/10.1002/jrsm.1439

Patel, P. (2022). *Optimized Approach for Isolation of Version Number Attack in IoT Systems*.

Popoọla, O. S. (2023). An Overview of the Evolutionary and Revolutionary Trends of Computer Network Intrusion and Detection. *SSRN*. https://doi.org/10.2139/ssrn.4532805

Pu, C. (2020). Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses. *IEEE Internet of Things Journal*, *7*(6), 4937–4949. https://doi.org/10.1109/jiot.2020.2971463

Pushpalatha, M., Anusha, T., Rama Rao, T., & Venkataraman, R. (2021). L-RPL: RPL powered by laplacian energy for stable path selection during link failures in an Internet of Things network. *Computer Networks*, *184*, 107697. https://doi.org/10.1016/j.comnet.2020.107697

Raghavendra, T., Anand, M., Selvi, M., Thangaramya, K., Santhosh Kumar, S., & Kannan, A. (2022). An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things. *Procedia Computer Science*, *215*, 61–70. https://doi.org/10.1016/j.procs.2022.12.007

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. *Sensors*, *22*(19), 7433. https://doi.org/10.3390/s22197433

Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. *IEEE Access*, *8*, 23022–23040. https://doi.org/10.1109/access.2020.2970118

Shirafkan, M., Shahidienjad, A., & Ghobaei-Arani, M. (2022). An autonomous intrusion detection system for the RPL protocol. *Peer-to-Peer Networking and Applications*, *15*(1), 484–502. https://doi.org/10.1007/s12083-021-01255-7

Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A., & Buchanan, W. J. (2020). Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL). *IEEE Access*, *8*, 43665–43675. https://doi.org/10.1109/access.2020.2977476

Zahra, F., Jhanjhi, N., Brohi, S. N., Khan, N. A., Masud, M., & AlZain, M. A. (2022). Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning. *Sensors*, *22*(18), 6765. https://doi.org/10.3390/s22186765

Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: Securing Internet of Things against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism. *Wireless Personal Communications*, *114*(2), 1287–1312. https://doi.org/10.1007/s11277-020-07421-z